REMARKS

Claims 1 to 23 are rejected.

Claims 1 to 23 remain in the application. Claims 1-14 and 18-20 have been amended.

Claims 1-7, 9, 11-14, and 18-20 have been amended in order to avoid invoking 35 U.S.C. 112, sixth paragraph. In particular, all instances of phrases such as --the steps of-- have been deleted. Applicant wishes to note for the record that the amendments are neither narrowing, nor are the amendments being made for a reason substantially related to patentability. Applicant respectfully submits that no new matter has been added in the amendments.

Specification

Paragraphs **[0032]** and **[0034]** have been changed to remove a clerical error.

Examiner has suggested that the title of the present application be changed to: "Method for securely supporting password change" from "Method for Supporting Single Sign On." Applicant has carefully considered the suggested title however; Applicant feels that the present title is more descriptive of the invention than the title proposed by Examiner. Applicant requests that Examiner carefully consider the material of paragraphs 36 and 37 of the present application as justification for the current title.

Claim Rejections – 35 USC § 102

Claim 1 has been amended to resolve errors in antecedence. In the cited reference of US patent 5,944,825 by Bellemore et al. (Bellemore.) Bellemore teaches a system that features a device that receives passwords and determines if they are acceptable prior to providing them to a password database. Bellemore does not specifically describe "storing data indicative of the new password in a database other than a password database". While Bellemore is unclear regarding what happens to a proposed password after having been evaluated for suitability a person of skill in the art would assume that copies of passwords that are suitable would be purged from the memory of the device used to evaluate the proposed password. A person of skill in the art will appreciate that if the memory is not purged then the additional copy of the password represents a potential security flaw in the system. Additionally, if the password is unsuitable then the unsuitable password should not be stored in the password database according to the teaching of Bellemore simply because an unauthorized user who gains access to a series of rejected passwords is likely to recognize a pattern in terms of user preferences for authentication codes. Thus, it is apparent that Bellemore does not teach "storing data indicative of the new password in a database other than a password database" as recited in independent claim 1. Therefore, the cited reference of Bellemore does not anticipate claim 1. Additionally, Bellemore does not suggest, "storing data indicative of the new password in a database other than a password database" as recited in claim 1 and therefore claim 1 is not obvious in light of Bellemore.

Claim 2 has been rejected as being anticipated by Bellemore. Claim 2 depends from claim 1 and, since claim 1 is not anticipated or obvious in light of Bellemore, claim 2 cannot be either of anticipated or obvious in light of Bellemore.

Claim 3 has been rejected as being anticipated by Bellemore. Claim 3 has been amended to clearly recite that the authorization data is not the password. Amended claim 3 recites, "...prompting a user to provide authorization data, the authorization data being other than

the password; and, associating the authorization data with the new password." The cited reference of Bellemore does not teach or suggest associated authorization data with the password, unless one were to consider the case of the authorization data being the password, which is clearly outside the scope of amended claim 3. Examiner has indicated that these steps are described in Bellemore however, after reviewing Bellemore and providing special attention to the cited passages, (Bellemore col. 2, lines 34-41, col. 4, lines 20-42 and col. 7, lines 4-19) Applicant is unable to appreciate Examiner's reasoning. Amended claim 3 depends from claim 1. As claim 1 is not anticipated by Bellemore, amended claim 3 cannot be anticipated by Bellemore.

Claim 4 has been rejected as being anticipated by Bellemore. Claim 4 clearly states: "...wherein detecting the new password comprises detecting the new password at least two separate times." Applicant has reviewed the cited reference of Bellemore and paid special attention to the referenced section of Bellemore regarding "detecting the new password at least two times" (Bellemore col. 3 line 56 to col. 4 line 42.) Applicant was unable to identify the relevance that Examiner has placed on this section of Bellemore to the limitations in scope recited in claim 4. Additionally claim 4 depends from claim 1. As claim 1 is not anticipated by Bellemore, claim 4 cannot be anticipated by Bellemore.

Claim 5 has been rejected as being anticipated by Bellemore. Independent claim 5 has been amended for clarity and improved antecedence. Amended independent claim 5 now recites:

> "detecting a change password operation in execution on a system for changing a first password;
>
> displaying to a user a prompt for a new password in response to detecting the change password operation in execution and other than occurring as an operation of the change password operation..."

The cited reference of Bellemore teaches a system that reviews passwords to determine if they meet certain predetermined criteria. Unlike amended independent claim 5 Bellemore does not teach displaying to a user a prompt for a new password "in response to detecting the change password operation in execution..." Specifically, Bellemore does not teach or suggest providing a prompt to a user when an operation to change a password is detected. Instead Bellemore incorporates a more conventional system in which a change password operation itself provides a prompt the user. Therefore, Bellemore does not anticipate amended independent claim 5. Similarly, the cited reference of Bellemore does not render amended independent claim 5 obvious.

Claim 6 has been rejected as being anticipated by Bellemore. Claim 6 depends from amended independent claim 5, which is neither anticipated nor obvious in light of Bellemore. Therefore, claim 6 cannot be either of anticipated or obvious in light of Bellemore.

Independent claim 7 has been rejected as being anticipated by Bellemore. Independent claim 7 has been amended to correct clerical errors that could cause confusion with regards to the scope of the claim. Additionally, claim 7 has been amended to eliminate inconsistencies in antecedence. Examiner has indicated that "storing the new password in a database independent of the change password operation and the data where the changed password is stored" is taught by "(Bell col. 6 line 11-36, col. 7 lines 4-19)." Applicant respectfully disagrees. In col. 6, lines 11-36 of Bellemore a method for preventing access by a user who was recently an authorized user but is now an unauthorized user is described. This is achieved by "updated the account_status to a value indicated that the user account is permanently locked." (Bellemore col. 6, lines 23 and 24) It is uncertain how a change in account status could be viewed as equivalent to changing a password. Specifically, changing account status does not change a password. In Bellemore, col. 7 lines 4-19 read,

"In step 405, a script of plurality of scripts is executed. Security process 204 transmits a message to script executing process 205. The message transmitted to script executing process 205 includes the user ID, the proposed password, and the current password. Script executing process 205 executes the script represented by field the verification.sub.-- script in the user profile table 207. Script executing process transmits a message to security process 204 indicating whether the proposed password meets the criteria embodied in the script."

Applicant asserts that transferring data and evaluating a password in a script as described in the cited text is not equivalent to "storing the new password in a database independent of the change password operation and of the database where a changed password is stored" as recited in amended independent claim 7. Having carefully reviewed the cited reference of Bellemore, Applicant is unable to find anything therein that could reasonably be considered equivalent to "storing the new password in a database independent of the change password operation and of the database where a changed password is stored" as recited in independent claim 7. Therefore Bellemore does not anticipate independent claim 7. Similarly, Bellemore does not render independent claim 7 obvious. Specifically, Bellemore describes a system that evaluates passwords (presumably) to ensure that they are secure. Additionally, Bellemore does not teach or suggest,

> "...detecting a password change operation in execution on a system;
> displaying to a user a prompt for authentication information in response to detecting the change password operation in execution and other than occurring as an operation of the change password operation ..."

Bellemore does not teach or suggest the method of independent claim 7 and, therefore, amended independent claim 7 is not anticipated or obvious in light of Bellemore. Thus,

amended independent claim 7 is allowable.

Claim 11 has been rejected as being anticipated by Bellemore. Claim 11 depends from independent claim 7, which is not anticipated or obvious in light of Bellemore. Therefore, claim 11 cannot be either of anticipated or obvious in light of Bellemore.

Claim 18 has been rejected as being anticipated by Bellemore. Claim 18 clearly recites, "performing another operation to change another password of the known user to the new password." Examiner has indicated that this step is described in the cited passage of Bellemore (Bellemore col. 7, lines 5-19):

> "In step 405, a script of plurality of scripts is executed. Security process 204 transmits a message to script executing process 205. The message transmitted to script executing process 205 includes the user ID, the proposed password, and the current password. Script executing process 205 executes the script represented by field the verification_script in the user profile table 207. Script executing process transmits a message to security process 204 indicating whether the proposed password meets the criteria embodied in the script.
>
> In step 410, a determination is made by security process 204 of whether execution of the verification script transmitted success or failure. In step 499, a message indicating whether the password and user ID combination is valid is transmitted to database management system 203, which in turn transmits the message to client 201."

Having carefully reviewed the cited passage, Applicant is unable to understand the logic of the argument presented by Examiner for rejection. The cited text does not specify or

suggest, "performing another operation to change another password of the known user to the new password" as recited in claim 18. Additionally, having reviewed the cited reference of Bellemore, Applicant was unable to locate any other portion of Bellemore that would render claim 18 either anticipated or obvious in light of Bellemore. Thus, claim 18 is neither anticipated nor obvious in light of Bellemore. Further, claim 18 depends from independent claim 7, which is neither anticipated nor obvious in light of Bellemore and, therefore, claim 18 cannot be either of anticipated or obvious in light of Bellemore.

Claim 19 has been rejected as being anticipated by Bellemore. Claim 19 has been amended to more clearly specify "determining within the password database and associated with a same user all passwords identical to the password being changed" instead of "all passwords identical to the password being changed" as originally stated in claim 19. Examiner has indicated that the limitations introduced in claim 19 are recited in Bellemore in a passage beginning on col. 8 line 46 and ending on col. 9 line 9. The passage cited by Examiner refers to a feature of Bellemore that stores copies of old passwords previously employed by the user. Thus, in Bellemore if a user is prompted to change their password but chooses to provide their current password or a recent used password instead of a "new" password then the system of Bellemore will recognize the old password and likely reject it. This is not consistent with what is described in amended claim 19. Specifically, amended claim 19 recites, "determining within the password database and associated with a same user all passwords identical to the password being changed and automatically performing at least another operation to change each identical password of the known user to the new password." Therefore, claim 19 is not anticipated by Bellemore. Additionally claim 19 depends from amended independent claim 7. Since amended independent claim 7 is neither anticipated nor obvious in light of Bellemore, claim 19 is neither anticipated nor obvious in light of Bellemore.

Claim 20 has been rejected under USC 102(b) as being anticipated by Bellemore (referred to as Bell by Examiner.) Regarding independent claim 20, Examiner asserted, "...Bell

teaches and describes a method of securely supporting password change comprising... automatically generated a new password (Bell column 1 lines 11-34 and column 7 lines 4-19)." Applicant respectfully disagrees. Having carefully reviewed the cited reference of Bellemore, applicant was unable to find any reference teaching or suggesting "automatically generating a new password". The "proposed password" described by Bellemore appears to be provided as a direct response to a user input signal. The cited reference of Bellemore teaches a system that goes to significant lengths to verify if the "proposed password" is acceptable. Clearly, if the proposed password were generated automatically, it would be a simple matter to ensure that an automatically generated password meets certain criteria by simply providing that method that cannot generate an unacceptable password. Clearly, this is not the case in Bellemore. As such it is apparent that Bellemore does not teach "automatically generating a password" and, therefore, it is apparent that claim 20 is not anticipated by Bellemore. Additionally, the cited reference of Bellemore fails to teach or suggest

> "detecting a password change operation in execution on a system having a known user authorized thereon;
> automatically generating a new password in response to detecting the password change operation and other than occurring as an operation of the change password operation..."

Therefore, it is apparent that claim 20 is neither anticipated nor obvious in light of Bellemore.

Claim Rejections – 35 USC § 103

Claim 8 has been rejected as being obvious in light of Bellemore in combination with Novoa. As described with reference to claim rejections made under 35 USC § 102, amended independent claim 7 is neither obvious nor anticipated in light of Bellemore. The

cited reference US patent 6,636,973 by Novoa et al. (Novoa) teaches a system that uses biometric authentication. Novoa teaches that each time a user authenticates, a password associated with that user is changed but that the new password is associated with data relating to the biometric data of the user. The cited reference of Novoa does not teach or suggest,

> "...detecting a password change operation in execution on a system;
>
> displaying to a user a prompt for authentication information in response to detecting the change password operation in execution..." as recited in amended independent claim 7.

Instead, Novoa teaches that the password change operation is part of a standard authentication process. As such, it is clear the password change operation of Novoa need not be "detected". Neither Bellemore nor Novoa teach or suggest "detecting a password change operation." Further, neither Bellemore nor Novoa teach or suggest, "displaying a user prompt for authentication information in response to detecting the change password operation in execution." Therefore, amended independent claim 7 is not obvious in light of the combination of Bellemore and Novoa.

Claims 8, 9 and 10 have been rejected as being obvious in light of the combination of Bellemore and Novoa. Since amended independent claim 7 is not obvious in light Bellemore in combination with Novoa claims 8, 9 and 10, which depend for amended independent claim 7 are not obvious in light of the same combination of cited references.

Claim 12 has been rejected as being obvious in light of the combination of Bellemore and Novoa. Claim 12 clearly states, "...wherein performing an operation to change the password comprises prompting the user to select between provision of the new password

and automatic generation of the new password." Bellemore does not teach or suggest providing the user the choice of provision of a new password and automatic generation of a new password. Instead, Bellemore teaches that the user provides the new password and the new password is tested to ensure that it is acceptable. Novoa does not teach or suggest providing the user the choice of provision of new password and automatic generation of a new password. Instead Novoa automatically provides a new password regardless of the user's preference. It is unclear why a person of skill in the art having reviewed and understood both Bellemore and Novoa would consider "prompting the user to select between provision of the new password and automatic generation of the new password" as recited in claim 12. Therefore, Applicant asserts that there is insufficient motivation to combine the cited references. Additionally, claim 12 depends from amended independent claim 7, which is not obvious and therefore claim 12 is not obvious.

Claims 13 and 15 has been rejected as being obvious in light of the combination of Bellemore and Novoa. Claims 13 and 15 depend from both claim 12 and amended independent claim 7. Since both claim 12 and claim 7 are not obvious in light of the cited combination of references it is apparent that claims 13 and 15 are not obvious in light of the same combination of cited references.

Claim 14 has been rejected as being obvious in light of the combination of Bellemore and Novoa. Claim 14 depends amended independent claim 7. Since claim 7 is not obvious in light of the cited combination of references it is apparent that claim 14 is not obvious in light of the same combination of cited references.

Claim 21 has been rejected as being obvious in light of the combination of Bellemore and Novoa. Amended independent claim 20 clearly recites,

"detecting a password change operation in execution on a system having a known

user authorized thereon;

automatically generating a new password in response to detecting the password change operation and other than occurring as an operation of the change password operation..."

As explained in arguments regarding anticipation of claim 20 by Bellemore, Bellemore does not teach this. Further, Novoa does not teach the cited text of amended independent claim 20. Specifically, while Novoa does teach generating a new password automatically, the generation of the password does not occur as a result of "detecting a password change operation" but instead is a regular operation of a password change operation. Examiner's attention is drawn to flowchart Fig. 4, item 346 of Novoa, which clearly occurs as a critical part of a password change operation. Therefore, claim 20 is not obvious in light of Novoa. As neither Bellemore nor Novoa teach the cited portion of amended independent claim 20 it is apparent that amended independent claim 20 is not obvious in light of the combination of Bellemore and Novoa. Therefore, it is clear that claim 21, which depends from claim 20 cannot be obvious in light of the combination of Bellemore and Novoa.

Claims 16, 17, 22 and 23 have been rejected as being obvious in light of Bellemore in combination with Novoa and US patent 5, 944,825 by Schneier (Schneier). As previously explained with respect to arguments regarding anticipation of claims 7 and 20 Bellemore does not teach or suggest,

"...detecting a password change operation in execution on a system...

displaying to a user a prompt for authentication information in response to detecting the change password operation in execution and other than occurring as an operation of the change password operation..."

Similarly, Novoa does not teach this instead, Novoa provides a password automatically as part of a change password operation, instead of "other than occurring as an operation of the change password operation." The cited reference of Schneier does not appear to teach such steps either. Instead, as described by Examiner, Schneier teaches that values generated by variable inputs are optionally used as encryption keys. As such, it is very clear that amended independent claim 7 is not obvious in light of Bellemore in combination with Novoa and Schneier. As claims 16 and 17 are dependent from claim 7 it is clear that this cited combination of references does not render claims 16 and 17 obvious. Further, having reviewed the arguments provided by Examiner, Applicant feels that it is unclear why the cited combination of references, having been read and understood by a person of ordinary skill in the art, would lead that person to the method of any of claims 7, 16 and 17.

Similarly, amended independent claim 20 states,

> "detecting a password change operation in execution on a system having a known user authorized thereon;
> automatically generating a new password in response to detecting the password change operation and other than occurring as an operation of the change password operation..."

These operations are clearly a subset of the similar operations of amended independent claim 7. These operations are not present or suggested in any of Bellemore, Novoa and Schneier. Therefore, Applicant is again confused regarding how a person of skill in the art would be lead to combine them to produce the method of amended independent claim 20. Additionally, even if these cited references could be combined to provide the method of amended independent claim 20 it is uncertain what motivation to combine the references exists. Although the references cited by Examiner all relate to security in computer networks, it is uncertain what else they have in common. For example, Applicant is unable to find anything anywhere in Bellemore that would lead one of skill in the art to consider

the material of Novoa and Schneier as being suitable for integration in Bellemore to produce methods according to claim 20. Applicant asserts that there is no clear traceable connection between the references other than the fact that they relate to computer security. Therefore it is clear that a person of skill in the art would not be lead to a method consistent with the method of amended independent claim 20 in light of the combination of Bellemore, Novoa and Schneier. Therefore claims 22 and 23, which depend from amended independent claim 20 are not obvious.

No new matter has been added.

A Petition for Extension of Time is filed concurrently with this response.

Please charge any additional fees required or credit any overpayment to Deposit Account No. 50-1142.

Applicant requests favourable reconsideration of the amended application.

Respectfully submitted,

Gordon Freedman, Reg. No. 41,553

Freedman and Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario
K2G 5X3 Canada

Tel (613) 274-7272
Fax (613) 274-7414

VL/sah